IN THE CLAIMS

1. (Currently Amended) A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the configuration data associated with an intellectual property block for implementing user logic on the configurable device, wherein the user logic includes functions associated with a user design for implementation on the configurable device;

disabling user logic provided for implementation of the configuration data after it is loaded onto the configurable device, wherein an error bit is set by a disabling signal generator to disable user logic;

generating a configurable device authorization code;

generating a secure device authorization code;

comparing the configurable device authorization code and the secure device authorization code; and

enabling the user logic if the configurable device authorization code corresponds to the secure device authorization code.

2. (Original) The method of Claim 1 wherein:

generating the configurable device authorization code comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the configurable device; and

generating the secure device authorization code comprises:

generating a second sequence in a pseudo-random number generator in the secure device;

transmitting the second sequence to an encryptor in the secure device;

encrypting the second sequence to generate a third sequence;

transmitting the third sequence to a decryptor in the configurable device; and

decrypting the third sequence to generate a fourth sequence, wherein the fourth sequence is the secure device authorization code.

3. (Original) The method of Claim 2 wherein the configurable device is an SRAM PLD.

4. (Original) The method of Claim 2 wherein the secure device is an EEPROM PLD.

5. (Original) The method of Claim 2 wherein the pseudo-random number generator in the secure device is a duplicate of the pseudo-random number generator in the configurable device and both pseudo-random number generators are seeded using the same seed.

6. (Original) The method of Claim 1 wherein:

generating the configurable device authorization code comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the configurable device; and

generating the secure device authorization code comprises generating a second sequence as the secure device authorization code in a pseudo-random number generator in the secure device.

7. (Original) The method of Claim 6 wherein the configurable device is an SRAM PLD.

8. (Original) The method of Claim 6 wherein the secure device is an EEPROM PLD.

9. (Original) The method of Claim 6 wherein the pseudo-random number generator in the secure device is a duplicate of the pseudo-random number generator in the configurable device and both pseudo-random number generators are seeded using the same seed.

10. (Original) The method of Claim 1 wherein:

generating the configurable device authorization code comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the configurable device;

generating the secure device authorization code comprises:

transmitting the first sequence to an encryptor in the secure device;

encrypting the first sequence to generate a second sequence;

transmitting the second sequence to a decryptor in the configurable device; and

decrypting the second sequence to generate a third sequence, wherein the third sequence is the secure device authorization code.

11. (Original) The method of Claim 10 wherein the configurable device is an SRAM PLD.

12. (Original) The method of Claim 10 wherein the secure device is an EEPROM PLD.

13. (Original) The method of Claim 1 wherein:

generating the secure device authorization code comprises generating a first sequence as the secure device authorization code in a pseudo-random number generator in the secure device;

generating the configurable device authorization code comprises:

transmitting the first sequence to an encryptor in the secure device;

encrypting the first sequence to generate a second sequence;

transmitting the second sequence to a decryptor in the configurable device; and

decrypting the second sequence to generate a third sequence, wherein the third sequence is the configurable device authorization code.

14. (Currently Amended) A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the configuration data associated with an intellectual property block for implementation using user logic on the configurable device, wherein the user logic includes functions associated with a user design for implementation on the configurable device;

disabling user logic provided for implementation of the configuration data after it is loaded onto the configurable device;

generating a configurable device authorization code using the configurable device sequence generator;

generating a first sequence in a secure device sequence generator in the secure device;

encrypting the first sequence in an encryptor in the secure device to generate a second sequence;

transmitting the second sequence to a decryptor in the configurable device;

decrypting the second sequence to generate a third sequence;

comparing the secure device authorization code and the configurable device authorization code; and

enabling the user logic if the configurable device authorization code corresponds to the secure device authorization code.

15. (Currently Amended) A method for controlling use of configuration data comprising:

programming a configurable device using the configuration data provided by a secure device, the configuration data associated with an intellectual property block for implementation using user logic on the configurable device, wherein the user logic includes functions associated with a user design for implementation on the configurable device;

disabling user logic provided for implementation of the configuration data after it is loaded onto the configurable device, wherein an error bit is set by a disabling signal generator to disable user logic;

generating a configurable device authorization code in the configurable device authorization code generator;

generating a secure device authorization code in a secure device authorization code generator in the secure device;

comparing the configurable device authorization code and the secure device authorization code; and

enabling the user logic if the configurable device authorization code corresponds to the secure device authorization code.

16. (Canceled)

17. (Currently Amended) A system for controlling use of configuration data, the system comprising a secure device and a configurable device, the system further comprising:

user logic in the configurable device, wherein the user logic includes functions associated with a user design for implementation on the configurable device, the user logic implemented using configuration data associated with an intellectual property block and disabled upon implementation on the configurable device;

a secure device authorization code generator configured to generate and transmit a secure device authorization code as a first input to the comparator;

a configurable device authorization code generator configured to generate and transmit a configurable device authorization code as a second input to the comparator;

wherein user logic is enabled if the secure device authorization code corresponds to the configurable device authorization code.

18. (Original) The system of Claim 17 wherein:

the configurable device generator comprises a sequence generator in the configurable device; and the secure device generator comprises:

a sequence generator in the secure device;

an encryptor coupled to the secure device sequence generator and configured to encrypt a first sequence generated by the secure device sequence generator to generate a second sequence; and

a decryptor in the configurable device, the decryptor coupled to the encryptor and configured to decrypt the second sequence to generate a third sequence and to transmit the third sequence as the secure device authorization code to the first input of the comparator.

19. (Original) The system of Claim 18 wherein the configurable device sequence generator and the secure device sequence generator are pseudo-random number generators and further wherein the configurable device pseudo-random number generator is a duplicate of the secure device pseudo-random number generator.

20. (Original) The system of Claim 18 wherein the configurable device is an SRAM PLD.

21. (Original) The system of Claim 18 wherein the secure device is an EEPROM PLD.

22. (Original) The system of Claim 19 wherein the pseudo-random number generators are seeded using the same seed.

23. (Original) The system of Claim 17 wherein:

the configurable device authorization code generator comprises a sequence generator in the configurable device; and

the secure device authorization code generator comprises a sequence generator in the secure device.

24. (Original) The system of Claim 23 wherein the configurable device sequence generator and the secure device sequence generator are pseudo-random number generators and further wherein the configurable device pseudo-random number generator is a duplicate of the secure device pseudo-random number generator.

25. (Original) The system of Claim 23 wherein the configurable device is an SRAM PLD.

26. (Original) The system of Claim 23 wherein the secure device is an EEPROM PLD.

27. (Original) The system of Claim 24 wherein the pseudo-random number generators are seeded using the same seed.

28. (Original) The system of Claim 17 wherein:

the configurable device authorization code generator comprises a sequence generator in the configurable device configured to generate a first sequence as the configurable device authorization code; and

the secure device authorization code generator comprises:

an encryptor in the secure device, the encryptor configured to receive and encrypt the first sequence to generate a second sequence; and

a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence and to transmit the third sequence as the secure device authorization code to the comparator.

29. (Original) The system of Claim 28 wherein the configurable device sequence generator is a pseudo-random number generator.

30. (Original) The system of Claim 28 wherein the configurable device is an SRAM PLD.

31. (Original) The system of Claim 28 wherein the secure device is an EEPROM PLD.

32. (Original) The system of Claim 17 wherein:

the secure device authorization code generator comprises a sequence generator in the secure device configured to generate a first sequence as the secure device authorization code; and

the configurable device authorization code generator comprises:

an encryptor in the secure device, the encryptor configured to receive and encrypt the first sequence to generate a second sequence; and

a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence and to transmit the third sequence as the configurable device authorization code to the comparator.

33-50. (Canceled)